UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/582,803	06/14/2006	Yuichi Futa	2006_0892A	4687

52349 7590 12/05/2008

WENDEROTH, LIND & PONACK L.L.P.
2033 K. STREET, NW
SUITE 800
WASHINGTON, DC 20006

EXAMINER	
NGUYEN, MINH DIEU T	
ART UNIT	PAPER NUMBER
2437	
MAIL DATE	DELIVERY MODE
12/05/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/582,803	FUTA ET AL.	
	Examiner	Art Unit	
	MINH DIEU NGUYEN	2437	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *18 November 2008*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-15 and 18-23* is/are pending in the application.

4a) Of the above claim(s) *16 and 17* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-9, 11-15 and 18-23* is/are rejected.

7)☒ Claim(s) *10* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This office action is in response to the communication dated 11/18/2008.

2. Claims 1-15 and 18-23 are pending. Claims 16-17 are being withdrawn as being directed to a non-elected invention.

Claim Objections

3. Claims 1-2, 5, 10, 14, 18 and 20-21 are objected to because of the following informalities:

a) As to claim 1, the phrase "a random information generation unit operable to read the management information from the management information storage unit, and generate random information R based on the read management information" should be -- a random information generation unit operable to read the **unique** management information from the management information storage unit, and generate random information R based on the read **unique** management information --.

b) As to claims 2, 5, 10, 14, 18, 20 and 21, same issue like claim 1.

Appropriate correction is required.

Claim Rejections - 35 USC § 101

4. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

5. Claims 20-21 and 23 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. Claim 20 recites a prime calculation method of outputting a prime once the primality of the prime is determined, however it lacks producing a useful result in order to accomplish a practical application. As such, it fails to fall within a statutory category. Claim 21 lacks the necessary physical articles or objects to constitute a machine or a manufacture within the meaning of 35 U.S.C. 101. It is clearly not a series of steps or acts to be a process nor is it a combination of chemical compounds to be a composition of matter. As such, it fails to fall within a statutory category. It is, at best, functional descriptive material per se. Claim 23 recites the prime-calculation computer program to be transmitted on a carrier wave. Carrier wave is a signal, not a series of steps. Carrier wave is a form of energy and not a composition of matter. Carrier wave does not have any physical structure and thus does not fit within the definition of a machine or an article of manufacture. It also fails to fall within a statutory category.

Double Patenting

6. The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. A nonstatutory obviousness-type double patenting rejection is appropriate where the conflicting claims are not identical, but at least one examined application claim is not patentably distinct from the reference claim(s) because the examined application claim is either anticipated by, or would have been obvious over, the reference claim(s). See, e.g., *In re Berg*, 140 F.3d 1428, 46 USPQ2d 1226 (Fed. Cir. 1998); *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422

F.2d 438, 164 USPQ 619 (CCPA 1970); and *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) or 1.321(d) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent either is shown to be commonly owned with this application, or claims an invention made as a result of activities undertaken within the scope of a joint research agreement.

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

7. Claims 1-15 and 18-23 are provisionally rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 1-36 of copending Application No. 10/582999. Although the conflicting claims are not identical, they are not patentably distinct from each other because they are directed to the same invention in achieving prime calculation where producing identical primes is avoided.

This is a provisional obviousness-type double patenting rejection because the conflicting claims have not in fact been patented.

Claim Rejections - 35 USC § 103

8. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

9. Claims 1-9, 11-15, 18, 20-23 are rejected under 35 U.S.C. 103(a) as being unpatentable over Applicant Admitted Prior Art (AAPA) in view of Peyravian et al. ("Generation of RSA Keys That Are Guaranteed to be Unique for Each User).

a) As to claims 1, 20 and 21-23, AAPA discloses a prime calculating apparatus for calculating a prime candidate N larger than a known prime q and testing primality of the calculated prime candidate N, comprising:

a prime storage unit storing the known prime q; a random information generation unit operable to generate random information; a candidate calculation unit operable to read the prime q from the prime storage unit, and calculate the prime candidate N according to N= 2 x random information R x prime q + 1; a primality testing unit operable to test primality of the calculated prime candidate N; and an output unit operable to output the calculated prime candidate N as a prime N when the primality of the calculated prime candidate N is determined (AAPA: 0024-0030). AAPA is silent on the capability of having unique management information and generating random information R based on the unique management information. Peyravian is relied on for the teaching of having unique management information and generating random information R based on the unique management information (Peyravian: sections 2-4). It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of having unique management information and generating random information R based on the unique management information in the system of AAPA, as Peyravian teaches, so as to offer much stronger uniqueness and protection to system.

b) As to claims 2-3, the combination of AAPA and Peyravian discloses the random information generation unit includes: a reading subunit operable to read the unique management information from the management information storage unit; a random number calculation unit operable to calculate a random number r; a combining

subunit operable to make a combination of the read unique management information and the generated random number r; and a computation subunit operable to compute the random information R based on the combination by applying an injection function to the combination (Peyravian: section 3).

c) As to claim 4, exclusive-or function is a well-known, standard operation on bits. It can be used to XOR a plaintext with a keyword to generate a ciphertext. It is a designed choice to apply XOR function to the key information and the combination as claimed.

d) As to claim 5, the combination of AAPA and Peyravian discloses calculating the prime candidate N having a bit length twice a bit length of the prime q, wherein the random number calculation subunit calculates the random number r, a bit size of which is obtained by subtracting a bit length of the unique management information and 1 from the bit length of the prime q (i.e. random number r having length (q) -1 bit, random information R is a combination of random number r and management information as disclosed by Peyravian, therefore the bitsize of random number r is obtained by subtracting a bit length of the unique management information and 1 from the bit length of the prime q, AAPA: 0024).

e) As to claim 6, the combination of AAPA and Peyravian discloses the primality testing unit includes: a first judging subunit operable to judge whether the prime candidate N satisfies $2^{N-1} = 1 \bmod N$; and a second judging subunit operable to perform, when the judgment of whether the prime candidate N and the random

information R satisfy $2^{2R} \neq 1 \bmod N$, and to determine the primality of the prime candidate N when the performed judgment is affirmative (AAPA: 0030, 0032-0033).

f) As to claim 7, the combination of AAPA and Peyravian discloses the primality testing unit includes: a first judging subunit operable to judge whether the prime candidate N satisfies $2^{N-1} = 1 \bmod N$; and a second judging subunit operable to perform, when the judgment of whether the prime candidate N and the random information R satisfy GCD(2^{2R} -1, N) =1, and to determine the primality of prime candidate N when the performed judgment is affirmative (AAPA: 0027, 0028).

g) As to claims 8-9, the combination of AAPA and Peyravian discloses an iteration control unit operable to control the random information generation unit, the candidate calculation unit, and the primality testing unit to iterate the generation of the random information R, the calculation of the prime candidate N, and the primality testing until the primality of the calculated prime candidate N is determined by the primality testing unit (AAPA: 0029), the iteration control unit therefore iterates the random information R', calculates N'=2 x random information R' x prime N +1 and tests the primality of N' and continues with the iteration steps.

h) As to claim 11, the combination of AAPA and Peyravian discloses a key generating apparatus for generating a public key and a private key of RSA encryption, further comprising: a public key generation unit operable to generate the public key using the prime N; and a private key generation unit operable to generate the private key using the generated public key (AAPA: 0005, 0008).

i) As to claim 12, the combination of AAPA and Peyravian discloses the public key generation unit (i) directs the iteration control unit to newly obtain a prime N', (ii) calculates a number n, according to n=prime N x prime N', using the prime N and the newly obtained prime N', and (iii) generates a random number e, a combination of the calculated number n and the generated random number e is the public key, the private key generation unit calculates d satisfying e x d =1 mod L, L is a least common multiple of the prime N-1 and the prime N' -1, and the calculated d is the private key (AAPA: 0009-0014).

j) As to claim 13, the combination of AAPA and Peyravian discloses a key issuing server apparatus for generating and issuing the private key and the public key of RSA encryption for a terminal further comprising a key output unit operable to output the generated private key to the terminal; and a publishing unit operable to publish the generated public key (AAPA: 0004).

k) As to claims 14-15, the combination of AAPA and Peyravian discloses an identifier obtaining unit operable to obtain a terminal identifier uniquely identifying the terminal; a management information generation unit operable to generate the unique management information including the obtained terminal identifier; and a writing unit operable to write the generated management information to the management information storage unit, a server identifier storage unit prestoring a server identifier uniquely identifying the prime calculating apparatus functioning as the key issuing server apparatus, wherein the management information generation unit further reads the server identifier from the server identifier storage unit, and generates the unique

management information further including the read server identifier (Peyruvian: section 8).

l) As to claim 18, please see addressed above claim 1, 8 and 13.

10. Claim 19 is rejected under 35 U.S.C. 103(a) as being unpatentable over Applicant Admitted Prior Art (AAPA) in view of Peyravian et al. ("Generation of RSA Keys That Are Guaranteed to be Unique for Each User) and further in view of Oka et al. (2002/0108042).

The combination of AAPA and Peyravian is silent on the capability of having a certificate issuing server apparatus, wherein the key output unit outputs the public key to the certificate issuing server apparatus and the certificate issuing server apparatus includes: a storage unit storing a private key of the certificate issuing server apparatus; an obtaining unit operable to obtain the public key; a certificate generation unit operable to (i) generate signature data by applying a digital signature to public key information including the public key, using the private key of the certificate issuing server apparatus, and (ii) generate a public key certificate including at least the public key and the generated signature data; and an output unit operable to output the generated public key certificate to the key issuing server apparatus. Oka is relied on for the teaching of having a certificate issuing server apparatus, wherein the key output unit outputs the public key to the certificate issuing server apparatus and the certificate issuing server apparatus includes: a storage unit storing a private key of the certificate issuing server apparatus; an obtaining unit operable to obtain the public key; a certificate generation

unit operable to (i) generate signature data by applying a digital signature to public key information including the public key, using the private key of the certificate issuing server apparatus, and (ii) generate a public key certificate including at least the public key and the generated signature data; and an output unit operable to output the generated public key certificate to the key issuing server apparatus (Oka: 0001, 0018-0019, Fig. 2-3, 8). It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of having a certificate issuing server apparatus, wherein the key output unit outputs the public key to the certificate issuing server apparatus and the certificate issuing server apparatus includes: a storage unit storing a private key of the certificate issuing server apparatus; an obtaining unit operable to obtain the public key; a certificate generation unit operable to (i) generate signature data by applying a digital signature to public key information including the public key, using the private key of the certificate issuing server apparatus, and (ii) generate a public key certificate including at least the public key and the generated signature data; and an output unit operable to output the generated public key certificate to the key issuing server apparatus in the system of AAPA and Peyravian, as Oka teaches, so as to provide public key certificate for users.

Allowable Subject Matter

11. Claim 10 is objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Conclusion

12. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Minh Dieu Nguyen whose telephone number is 571-272-3873.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on 571-272-3865. The fax phone number for the organization where this application or proceeding is assigned is (571) 273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

/Minh Dieu Nguyen/
Primary Examiner, Art Unit 2437